UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

JON KAHEN, a/k/a JON KAEN, GLOBAL VOICECOM, INC., GLOBAL TELECOMMUNICATION SERVICES INC., and KAT TELECOM, INC.,

Defendants.

COMPLAINT

Civil Action No.

CV 20-00474

COGAN, J.

Plaintiff, the UNITED STATES OF AMERICA, by and through the undersigned attorneys, hereby alleges as follows:

INTRODUCTION

1. The United States brings this action for a temporary restraining order, preliminary and permanent injunctions, and other equitable relief pursuant to 18 U.S.C. § 1345, in order to enjoin the ongoing commission of criminal wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349. The United States seeks to prevent continuing and substantial injury to the victims of fraud.

2. Since at least 2017 and continuing through the present, Defendant John Kahen, a/k/a Jon Kaen ("Kaen"), together with one or more co-conspirators, has used the U.S. telephone system to engage in predatory wire fraud schemes that victimize individuals throughout the United States, including individuals within the Eastern District of New York and significant numbers of elderly and vulnerable victims. Kaen controls various corporate entities that he utilizes in furtherance of the fraudulent scheme, including Defendants Global Voicecom, Inc.; Global

Telecommunications Services Inc.; and KAT Telecom, Inc. (the "Corporate Defendants," and together with Kaen, the "Defendants). The Corporate Defendants, based in New York, are VoIP[1] carriers that serve as "gateway carriers"[2] facilitate the delivery of millions of fraudulent "robocalls"[3] every day from foreign call centers and foreign VoIP carriers to the U.S. telecommunications system and ultimately to phones throughout the United States. The Defendants thus provide foreign fraudsters the means to access the U.S. telephone system, knowingly passing millions of fraudulent robocalls intended to deceive the recipient into: (1) answering or returning the call, and (2) paying money to the perpetrators of the schemes.

3. Through these robocalls, fraudsters operating overseas impersonate government entities and well-known businesses by "spoofing"[4] legitimate phone numbers and sending recorded messages that are transmitted across the internet to telephones throughout the United States. These robocalls purport to be from federal government agencies, elements of foreign governments, and legitimate businesses, conveying alarming messages, such as that the call recipient's social security number or other personal information has been compromised or otherwise connected to criminal activity; the recipient faces imminent arrest; the recipient's assets are being frozen; the recipient's bank and credit accounts have suspect activity; the recipient's

---

[1] VoIP stands for voice-over-internet protocol and allows users to place phone calls over a broadband internet connection.

[2] As set forth in further detail herein, "gateway" carriers are the first in a chain of VoIP carriers located in the United States that facilitate the delivery of foreign VoIP calls to receipients in the United States.

[3] "Robocall" means a call made through an automated process that places large volumes of telephone calls over the internet in order to deliver recorded messages, in contrast to calls placed one at a time by a live person.

[4] The practice of making a false number appear on the recipient's caller ID is known as "spoofing."

benefits are being stopped; the recipient faces imminent deportation; or combinations of these things—all lies intended to induce potential victims to speak to the fraudsters. When individuals answer the calls or return voicemail messages, the fraudsters offer to "resolve" these legal matters by immediate transfers of funds to settle the purported legal obligation, or to hold the individual's assets only temporarily while the crisis resolves. In reality, the individual is neither under investigation nor in legal jeopardy, and the same threatening robocall was made simultaneously to thousands of other U.S. telephones.

4. Not only do Defendants deliver vast numbers of fraudulent robocalls every day, but they also participate in the fraudulent schemes by providing return-calling services to the fraudsters used to establish contact with potential victims. Robocall messages will often provide domestic and toll-free call-back numbers; potential victims who call these numbers connect to the overseas fraudsters, who then try to extort and defraud the potential victims.

5. The Defendants profit from these fraudulent robocall schemes by receiving payment from their co-conspirators for the services Defendants provide. In addition, on at least one occasion Defendants received a direct payment from a victim of one of the fraudulent schemes.

6. Since 2017 and continuing through the present, as a result of their conduct, Defendants and their co-conspirators have defrauded numerous victims out of millions of dollars, including victims in the Eastern District of New York.

7. For the reasons stated herein, the United States requests injunctive relief pursuant to 18 U.S.C. § 1345 to enjoin Defendants' ongoing scheme to commit wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349.[5]

[5] This case is one of two cases being filed simultaneously in which the United States Department of Justice, for the first time, seeks to enjoin telecommunications companies from participating in robocalling fraud schemes pursuant to 18 U.S.C. § 1345.

JURISDICTION AND VENUE

8. The Court has subject matter jurisdiction over this action pursuant to 18 U.S.C. § 1345 and 28 U.S.C. §§ 1331 and 1345.

9. Venue lies in this district pursuant to 28 U.S.C. § 1391(b)(2).

PARTIES

10. Plaintiff is the United States of America.

11. Defendant Kaen resides in Nassau County, New York, in the Eastern District of New York. Kaen controls Defendants Global Voicecom, Inc., Global Telecommunication Services Inc., and KAT Telecom, Inc., which he uses in furtherance of the fraudulent robocall scheme. Kaen operates the Corporate Defendants as a single enterprise from his home in the Eastern District of New York. One or more of the Defendants also conducts business as "IP Dish."

12. Defendant Global Voicecom, Inc. is a New York corporation. The New York Department of State, Division of Corporations Entity Information database identifies Global Voicecom's principal executive office as being located in Great Neck, New York, in the Eastern District of New York, and Kaen as the corporation's Chief Executive Officer.

13. Defendant Global Telecommunication Services Inc. is a New York corporation. Global Telecommunication Service's principal place of business is located in Great Neck, New York, in the Eastern District of New York.

14. Defendant KAT Telecom, Inc. is a New York corporation. KAT Telecom's principal place of business is located in Great Neck, New York, within the Eastern District of New York.

OVERVIEW OF THE ROBOCALLING FRAUD SCHEMES

A. Robocalling Fraud Targeting Individuals in the United States

15. The robocalling fraud schemes in which the Defendants are engaged share the same characteristics. Individuals at call centers located abroad, many of which are operating out of India, are bombarding the U.S. telephone system every day with millions of robocalls intended to defraud individuals in the United States. Many of these fraudsters impersonate U.S. government officials, foreign government officials, or well-known American businesses, in order to threaten, defraud, and extort money from robocall recipients. Robocalling technology, which allows fraudsters to send millions of calls per day all transmitting the same pre-recorded, fraudulent message, enables fraudsters to cast a wide net for elderly and vulnerable victims who are particularly susceptible to the threatening messages the fraudsters are sending. Even if only a small percentage of the recipients of a fraudulent call center's robocalls connect with potential victims, the fraudsters can still reap huge profits from their schemes.

16. Foreign fraudsters operate many different schemes targeting individuals in the United States, but the Defendants' robocall schemes include the following categories of impersonation scams:

a. *Social Security Administration ("SSA") Imposters*: Defendants transmit recorded messages in which SSA imposters falsely claim that the call recipient's social security number has been used in criminal activity, the individual's Social Security benefits will be suspended, the individual has failed to appear before a grand jury and face imminent arrest, or the individiual's social security number will be terminated. When a call recipient calls back or connects to the fraudster, the fraudster claims to be an SSA employee and typically tells the individual to transfer substantial funds to the SSA for safekeeping until a new social security number can be issued, at which point the individual's funds purportedly will be returned.

b. *Internal Revenue Service ("IRS") and Treasury Imposters*: Defendants transmit recorded messages in which IRS imposters falsely claim that the call recipient has been implicated in tax fraud, the individual has avoided attempts to enforce criminal laws, the individual has avoided court appearances, or the individual faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS or Treasury employee and typically tells the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.

c. *United States Citizenship and Immigration Services ("USCIS") Imposters*: Defendants transmit recorded messages in which USCIS imposters falsely claim that the call recipient has failed to fill out immigration forms correctly, the individual faces imminent arrest or deportation, that the individual's home country has taken formal action that may result in deportation, or the individual has transferred money in a way that will result in deportation. When a call recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the individual to pay various fees or fines to avoid immigration consequences.

d. *Foreign Government Imposters*: Defendants transmit recorded messages in which foreign government imposters, often in foreign languages, falsely claim to be from the U.S.-based consulate of a foreign government and that the call recipient faces problems with immigration status or a passport. When a call recipient calls back or connects to the fraudster, the fraudster falsely claims that the individual must

pay various fees or fines in order to avoid immigration consequences such as deportation.

e. *Tech Support Imposters*: Defendants transmit recorded messages in which fraudsters operating tech support scams impersonate various well-known tech companies such as Apple or Microsoft, and falsely claim that the call recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster instructs the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.

17. These robocalls are often "spoofed" so that they falsely appear on a victim's caller ID to originate from U.S. federal government agency phone numbers, such as the SSA's main customer service number, from local police departments, 911, or from the actual customer service phone numbers of legitimate U.S. businesses. These "spoofed" numbers are used to disguise the origin of the robocalls and the callers' identities, and to cloak them with the authority of government agencies or large businesses to induce potential victims to answer or return the calls. In reality, the calls originate from fraudsters operating abroad, and have no connection to any U.S. government agency or other legitimate enterprise.

18. Individuals who answer or otherwise respond to these calls eventually speak to live fraudsters who tell the individuals lies intended to frighten and confuse them so that the fraudsters may begin to control their behavior and isolate them from authorities, friends, and family members. These lies often include that the individual's social security number or other personal information has been implicated in criminal activity, that the individual faces imminent arrest or deportation, and that the individual's assets are about to be forfeited to the government. Once an individual is

overcome by fear and panic, the fraudsters keep them on the phone and offer reassurances that the individual's purported legal problems can be resolved through payment of money, or that the individual's money must be transferred for safekeeping to the government agency the fraudsters are impersonating. The fraudsters often claim that the victim's payment will be returned to them in the immediate future. In reality, once the fraudsters are convinced they have extorted as much money as possible from the victim, they drop all contact, leaving the victim without meaningful recourse. Fraudsters receive victims' money through retail gift cards, bank wires, cash payments, cryptocurrency transfers, and other methods.

19. Since October 2018, the most prolific robocalling scam impersonating U.S. government officials—and one engaged in by Defendants—is impersonation of the SSA. For example, a robocall sent to millions of phones in the United States in early 2019 contained the following message:

> Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-[XXX]-[XXXX] I repeat 619-[XXX]-[XXXX] thank you.

20. SSA received more than 465,000 complaints about fraudulent telephone impersonation of the Administration from October 1, 2018 through September 30, 2019. Losses associated with these complaints exceed $14 million. Similarly, the Federal Trade Commission ("FTC") reported that for 2018, its Consumer Sentinel database received more than 39,000 fraud complaints about SSA imposter calls, with estimated losses of approximately $11.5 million; for 2019, the FTC reported that SSA imposter call complaints rose to approximately 166,000 with

associated losses of more than $37 million.[6] Complaint numbers substantially underrepresent the extent of the problem, because most victims do not report their losses to the government.

B. How Calls From Foreign Fraudsters Reach U.S. Telephones

21. The Defendants' robocalling fraud schemes, which involve robocalls that originate abroad and target individuals in the United States, are all dependent on VoIP and related technology to create the calls. VoIP calls use a broadband internet connection—as opposed to an analog phone line—to place telephone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional, wired phone. The robocalling fraud schemes also require U.S.-based telecommunications companies—referred to as "gateway carriers"—to introduce the foreign phone traffic into the U.S. phone system. A foreign call center or telecommunications company that places VoIP calls to U.S. telephones must have a relationship with a U.S. gateway carrier. From the gateway carrier, most VoIP calls will pass through a series of U.S.-based VoIP carriers before reaching a consumer-facing "common carrier" such as AT&T or Verizon, and ultimately a potential victim's phone. One of the Defendants' roles in the fraudulent schemes is to serve as a gateway carrier for the fraudulent robocalls.

22. Each provider in the chain that transmits a VoIP call maintains records, primarily for billing reasons, of all of the calls that pass through it. These records include the following information: the date and time of the call, the destination number (intended recipient), the source number from which the call was placed (sometimes a real number and sometimes a spoofed number), the name of the company that sent the call to the provider, and the downstream company to which the provider sent the call. These records are generated automatically as a call is routed

[6] Regarding government imposter fraud more broadly and not limited just to SSA imposters, the FTC's Consumer Sentinel database contains 255,223 complaints reflecting $128,479,054 in losses for 2018, and 389,563 complaints reflecting $152,946,623 in losses for 2019.

through telecommunications infrastructure in a manner that achieves the lowest cost to transmit a given call, known in the industry as "least-cost routing." Calls may be traced through these records back to their gateway carrier, and thus to their foreign source. The telecommunications industry refers to this tracing process as "traceback."

23. Tracebacks of many different robocalling fraud schemes have led to the identification of Defendants as a gateway carrier willing to transmit huge volumes of fraudulent robocalls into the country, despite clear indicia of fraud in the call traffic and actual notice of fraud.

DEFENDANTS' ONGOING PARTICIPATION IN ROBOCALLING FRAUD SCHEMES

24. Since at least 2017, the Defendants have knowingly provided U.S.-bound calling services to foreign fraudsters operating robocall scams, acting as a gateway carrier and passing robocalls into the U.S. telephone system by the millions. The Defendants are paid for each call they pass into and through the U.S. telephone system. In addition, the Defendants have provided return-calling services to the fraudsters operating the robocall scams, for which Defendants are also paid, enabling the fraudsters to establish contact with unwitting individuals after the individuals are deceived by a robocall.

25. There is substantial evidence of the Defendants' knowledge of the fraudulent nature of the calls they transmit, including call records showing high percentages of short-duration, unanswered calls[7] passing through their systems by the millions; thousands of spoofed calls purporting to be from "911" and similar numbers originating from overseas; dozens of complaints, warnings, and inquiries from vendors and other telecommunications companies about fraud, spoofing, and short-duration "junk" calls; repeated warnings and inquiries from an industry trade

[7] Short-duration and unanswered calls include calls where recipients immediately hang up and calls that do not connect because robocalls are sent to numerous telephone numbers that are not in service.

group about the scam robocalls passing through the Defendants' system; and receipt of numerous complaints from common-carrier telecommunications companies whose customers were victims of these fraud schemes.

A. Defendants Knowingly Introduce Fraudulent Robocalls into the U.S. Telephone System

26. In the telecommunications industry, high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. Defendants regularly transmit massive volumes of such calls. For example, the Government's investigation has revealed a sample of more than 7.7 million calls that Defendant Global Voicecom routed through a single downstream VoIP carrier over 19 days in May and June 2019, months after Kaen's response to the FCC. Of those calls, approximately 86%, more than 6.6 million calls, were one second or less in duration, indicating exceedingly high levels of junk and fraudulent robocalls. Moreover, a small sample of approximately 330,000 of these calls was examined in greater detail; of these approximately 330,000 calls in that 19-day period, more than 270,000 (approximately 81%) were from source numbers (the numbers appearing on the recipients' caller IDs) identified as fraudulent robocalls. Similarly, of the more than 106,000 robocalls spoofing the SSA's toll-free customer service number in January and February 2019 that Defendant Global Voicecom transmitted into the United States, nearly 60% had a call duration of less than one second, and another 38% were between one and 60 seconds in duration. During that same period in January and February 2019, Defendant Global Voicecom also ran through its systems thousands of calls spoofing 911, 1911, and 11911, with similar short call durations.

27. Since 2017, significant numbers of fraudulent robocalls have been traced back to the Defendants and brought to their attention. For example, U.S. common carrier AT&T has

notified Defendants on numerous occasions about fraud traced back to Defendants' operations. These notices include a November 16, 2017, email to IP Dish:

> The following calls to AT&T cell phone customers were received using the spoofed caller ID numbers of a non-working number at the US Department of Homeland Security headquarters. Callers impersonated US Citizenship and Immigration[ ] Services personnel and defrauded an AT&T customer of $1,450. . . .
> Pursuant to the customer and carrier network fraud protection provisions of the Telecommunication Act and the Telephone Records Privacy Protection Act (47 USC 222(d)(2)), could you provide the name(s) of your upstream carriers? We are tracing these calls to their source so they can be stopped.

AT&T sent similar emails about USCIS impersonation scams to Defendants Kaen and Global Voicecom in September 2017, November 2017, April 2018, and July 2018. Similarly, AT&T emailed Defendants about SSA and other imposter robocalls on January 29, 2019:

> We have been receiving AT&T customers complaints about spoofing fraud from your network. In the first complaint calls are originating from a toll free number owned by the US Social Security Administration. Callers falsely claim to be US Government officials and attempt to extort money from our customers. We have verified this number is not out-pulsed as a legitimate caller ID by the real US Social Security Administration. . . .
>
> In the second complaint calls are originating from the toll free number of DirecTV (AT&T). Callers falsely claim to be AT&T/DirecTV technical reps and social engineer remote access to our customer's computers in order to make fraudulent wire transfers from online banking applications. . . .
> Could you provide the names and contact numbers of the parties that sent these calls to your network.

AT&T sent similar warning notices about SSA imposter calls to Defendants Kaen and Global Voicecom in February 2019 and May 2019.

28. Another VoIP carrier that received call traffic from Defendants, Peerless Network, Inc., sent even more warning notices and inquiries to Defendants. For example, Peerless Network sent a warning notice about spoofed calls in September 2018 with a request that Defendants investigate and "take the appropriate action." Peerless Network sent approximately 12 of these warning notices between September 2018 and March 2019.

29. Not only have other telecommunications companies provided warnings and notices to Defendants as a result of tracebacks, but a leading industry trade group, USTelecom, has done the same. For example, USTelecom traced back an August 19, 2019 robocall that originated from India and came through Defendant Global Voicecom as the gateway carrier. The robocall was also routed through Defendant KAT Telecom. This robocall stated that there was "suspicious activity" associated with the individual's social security number. USTelecom provided the following warning notice in its correspondence to Defendant Global Voicecom on August 27, 2019:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI[8] is not effective.

Blocking specific telephone numbers is an ineffective means to stop fraudsters who are willing—and have the ready ability—to spoof any number as the caller ID number for their fraudulent robocalls. For example, in January and February 2019, Defendants transmitted fraudulent robocalls spoofing 911, 1911, and 11911. Nevertheless, if the Defendants responded at all to these notices and warnings from other telecommunications–industry actors, they routinely responded that the "offending" number had been blocked, as though the spoofed telephone number and not the caller were responsible for the fraud.

30. Similarly, USTelecom traced an October 3, 2019 robocall to Defendant Global Voicecom as the gateway carrier. This robocall also originated from India. USTelecom provided

[8] "ANI" means "Automatic Number Identification," and for these purposes refers to the purported source number for the call.

the following warning notice in its October 11, 2019 correspondence to Defendant Global Voicecom:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Calls placed from specific numbers obtained by scammers, using an automated voice to inform called party that they are in trouble with IRS and will be arrested. Called party is instructed to call back to speak to an agent. . . We are using traceback to try to find the source(s) of the millions of outbound calls that are being made to initiate the scam.

USTelecom's records indicate that this robocall was transcribed in part as follows:

> This call is from Federal Tax and audit division of internal revenue services. This message is intended to contact you regarding an enforcement action executed by the US treasury intending your serious attention. Ignoring this will be an intentional second attempt to avoid initial appearance before a magistrate judge or a grand jury for federal criminal offense. This is a final attempt to reach you to resolve this issue immediately and to speak to a federal agent to call us back on 510-[XXX]-[XXXX]. I repeat 510-[XXX]-[XXXX].

USTelecom identified Defendants as the gateway carrier for foreign fraudulent robocalls on at least eighteen other occasions in the latter half of 2019 alone, each time providing similar warning notices about the nature of the scam robocalls. USTelecom's records indicate that on nearly all of these 2019 tracebacks, the scam robocalls came from the same company in India.

31. Defendants transmitted another group of fraudulent robocalls that spoofed the phone number for a foreign government consulate in New York, New York. These calls conveyed foreign-language messages about problems with the individual's immigration status or passport. Like with SSA imposter robocalls and other U.S. government-imposter scams, individuals who returned the calls to the consulate imposters were told lies intended to frighten them and make them think there are imminent consequences for involvement in criminal activity, and that funds must be transferred to the fraudsters to resolve the matters. Like with the SSA imposter scams, once the fraudsters are convinced they have extorted as much money as possible, they drop all contact with the victim. In 2018, the FCC traced this consulate imposter scam back to Kaen and

IP Dish, who informed the FCC that the calls came from a Hong Kong entity that was making tens of thousands of calls per day. The FTC's Consumer Sentinel database reflects more than 1,000 complaints related to the spoofed phone number of the consulate. These complaints relate hundreds of thousands of dollars in victim losses. Defendants continue to conduct business with this Hong Kong entity more than a year later.

32. Despite these notices and numerous others, Defendants continue to pass fraudulent robocalls into the U.S. telephone system to millions of U.S. telephones every day.

B. Defendants Provide Return-Calling and Toll-Free Services for Robocall Schemes

33. Not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that potential victims can call them back. These toll-free and direct-inward-dial ("DID") telephone numbers[9] and related services are provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is actually a telephone number that Defendants register to an internet address designated by the foreign fraudsters. Thus, the DID and toll-free numbers can be used to ring telephones anywhere in the world.

34. While DID and toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. DID or toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing—deception. The DID and toll-free services provided by Defendants use VoIP technology to direct potential victims' return calls from

[9] As applicable to the fraud schemes, direct-inward-dial numbers are phone numbers with U.S. area codes that are routed to fraudulent call centers in foreign countries through VoIP technology.

the United States to the foreign fraudsters' call centers. The Defendants have knowingly provided hundreds of these DID and toll-free numbers and associated calling services to foreign robocall fraudsters.

1. DID Numbers Used to Further Robocalling Fraud Schemes

35. Like telephone numbers used to make U.S.-bound robocalls, DID numbers can be traced to identify their providers and users. This process was used to identify DID numbers provided by the Defendants for use in the fraudulent robocall schemes. For example, records obtained from one U.S. company demonstrate that it assigned 902 DID telephone numbers to Defendant Global Voicecom. Approximately 55% of these DID telephone numbers are associated with more than 28,000 complaints in the FTC's Consumer Sentinel database. One of the 902 DID telephone numbers appeared in a robocall sent to millions of U.S. telephones in early 2019:

> Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-[XXX]-[XXXX] I repeat 619-[XXX]-[XXXX] thank you.

At the time of the robocalls, this DID telephone number was assigned to Defendant Global Voicecom, which used that DID telephone number to provide return-calling services to the overseas fraudsters. Individuals who return calls like these put themselves in a pool of likely victims, insofar as the individuals self-select through belief that the message was sufficiently credible to warrant a return call. Upon returning the call to 619-[XXX]-[XXXX], individuals were told that they were speaking to SSA agents, who offered to resolve the purported problems that prompted the call by way of immediate payment of funds. In reality, the person speaking to the individual was a fraudster, unaffiliated with the U.S. government.

36. Beginning as early as September 2017 and continuing through the present, the U.S. company that assigned these 902 DID numbers to Defendants provided numerous warning notices about how the numbers were being used to perpetrate fraud. For example, that company provided the following warning notice to Defendant Global Voicecom on September 13, 2017 and included the substance of several complaints about fraud:

> The DID: 847[XXXXXXX] which we show assigned to you, is being used for fraudulent purposes. The US Treasury Department has provided us with a few complaints which are listed below. Because of the nature of the complaints, we have disabled this number on our network.
>
> I received a call from 484-[XXX]-[XXXX] claiming that I was a subject of Treasury Fraud. [T]hey said to call back at 847-[XXX]-[XXXX]. The call was received on Friday September 8th at 4 pm. I live in Philadelphia, in the EST zone. They claimed I would be sued if I did not call back.
>
> I received a voicemail message with an automated recording claiming to be from the US Dept. of Treasury regarding tax fraud in my name. The call back number was 847-[XXX]-[XXXX]. No one answered the return call. I recently submitted via mail my 3rd installment of 2017 taxes, so I hope nothing has gone wrong in the process of receiving my payment. Is this a known scam number? Thank you.
>
> The voice message states (Pre-recorded): "Treasury my badge number is 4874. The nature and purpose of this call is regarding an enforcement action which has been executed by the [U.S.] treasury department regarding tax fraud against your name. Ignoring this would be an intentional attempt to avoid initial appearance before the majesty does or exempt or enforce criminal offence. Before this matter goes to federal claim, court house, or before you get arrested. Kindly call us back as soon as possible. The number to reach us is 847-[XXX]-[XXXX], let me repeat the number 847-[XXX]-[XXXX]. Hope to hear from you soon before the charges are pressed against you. Thank you."

Through the course of the ensuing years, Defendants continued to receive numerous similar warning notices about DID numbers and related services they provide. Defendants effectively ignored the warnings and never terminated the fraudsters' access to DID numbers for return calls.

37. In the course of the Government's investigation, SSA OIG agents obtained from Global Voicecom call records for seven of the 902 DID numbers assigned to Defendant Global

Voicecom that are associated with SSA imposter robocalls. According to Defendants' own records, Defendants provided these seven DID numbers to the same Indian entity that Defendant Global Voicecom identified to USTelecom as the gateway carrier for numerous government imposter scam robocalls.

38. These DID call records reveal that more than 10 million calls were placed in 2019 from more than 4.5 million unique phone numbers to the 902 DID numbers assigned to Defendant Global Voicecom. More than 240,000 of these calls were from area codes for the Eastern District of New York.

2. Toll-Free Numbers Used to Further Robocalling Fraud Schemes

39. Records from the FTC demonstrate that Defendants Global Voicecom and Jon Kaen are associated with more than 1000 October 2019 SSA-imposter robocalls to the FTC's offices. These robocalls appeared to originate from a toll-free telephone number. Toll-free numbers work in a manner similar to DID numbers, but are structured differently by the FCC and telecommunications industry. Somos, Inc. is the FCC-designated national administrator of the U.S. toll-free calling system. Among other functions within the industry, Somos registers "responsible organizations" that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. On October 23 and 24, 2019, the FTC's offices received approximately 1,000 robocalls with the following recording:

> …social security on an immediate basis as your social has been found some suspicious for committing fraudulent activities across the United State. Before we go ahead and suspend your social security permanently, we want you to call us back on our department toll free number at 877-[XXX]-[XXXX]. I repeat 8-877-[XXX]-[XXXX]. Do not disregard this message, and call us back as soon as possible. Thank you.

The toll-free 877 number appeared on the FTC's caller ID as well as in the actual robocall message as the return-call number. On October 24, 2019, an FTC investigator contacted Somos to determine which responsible organization was associated with that toll-free number, which Somos duly provided. The FTC investigator then contacted that responsible organization, who informed the investigator that the number was assigned to Defendants Global Voicecom and Jon Kaen.

40. That responsible organization provided numerous notices to Defendants concerning the toll-free numbers assigned to Global Voicecom and how they were being used to facilitate robocalling fraud, doing so 37 times between March 2019 and October 2019. For example, on April 8, 2019, the responsible organization emailed Defendant Global Voicecom: "We received a scam complaint on the number 888-[XXX]-[XXXX] and were asked to disconnect it. We dialed this number and found it was someone impersonating Microsoft, and is still connected." Similarly, on June 11, 2019, the responsible organization emailed Defendant Global Voicecom: "Please know that we have rec[ei]ved a serious complaint on TFN 888-[XXX]-[XXXX], which we see i[s] assigned to your account. This number was reported as a part of an "Amazon Customer Support Scam." On August 26, 2019, the responsible organization emailed Defendant Global Voicecom: "Please note that we have received reports that 877-[XXX]-[XXXX] is being used to spoof Bank of America. Can you please look into this, inform us of your results and take action if necessary?" To each of the dozens of notices, Defendants responded to the effect that the "offending" number has been blocked, as if the spoofed telephone number and not the caller were committing fraud, but never that they terminated the sources of the fraudulent robocalls.

41. The FTC's Consumer Sentinel reflects more than 1,400 complaints associated with the toll-free numbers assigned to Defendant Global Voicecom.

HARM TO VICTIMS

42. Defendants' fraudulent schemes have caused substantial harm to numerous victims, including many victims located in the Eastern District of New York. It is estimated that Defendants and their foreign co-conspirators defrauded victims out of millions of dollars per year through fraudulent robocalls and return-calling services. If allowed to continue, these losses will continue to rise and result in further harm to victims.

43. In addition to the massive cumulative effect of these fraud schemes on U.S. victims, the harm can be devastating to individual victims. Victims have faced terrifying threats from fraudsters impersonating government officials and have lost substantial sums of money.

44. Defendants' fraudulent schemes are ongoing and wide-ranging. Absent injunctive relief by this Court, the Defendants will continue to cause injury to victims in this District and throughout the United States, and the victims' losses will continue to mount.

COUNT I

(18 U.S.C. § 1345 – Injunctive Relief)

45. The United States realleges and incorporates by reference paragraphs 1 through 44 of this Complaint as though fully set forth herein.

46. By reason of the conduct described herein, Defendants violated, are violating, and are about to violate 18 U.S.C. §§ 1343 and 1349 by executing or conspiring to execute schemes or artifices to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises with the intent to defraud, and in so doing, transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, writings, signs, signals, pictures, or sounds for the purpose of executing such schemes or artifices.

47. Upon a showing that Defendants are committing or about to commit wire fraud, conspiracy to commit wire fraud, or both, the United States is entitled, under 18 U.S.C. § 1345, to a temporary restraining order, a preliminary injunction, and a permanent injunction restraining all future fraudulent conduct and any other action that this Court deems just in order to prevent a continuing and substantial injury to the victims of fraud.

48. As a result of the foregoing, Defendants' conduct should be enjoined pursuant to 18 U.S.C. § 1345.

PRAYER FOR RELIEF

WHEREFORE, the plaintiff United States of America requests of the Court the following relief:

A. That the Court issue an order, pursuant to 18 U.S.C. § 1345, pending a hearing and determination on the United States' application for a preliminary injunction, that Defendants, their agents, officers and employees, and all other persons and entities in active concert or participation with them are temporarily restrained from:

i. committing and conspiring to commit wire fraud, as defined by 18 U.S.C. §§ 1343 and 1349;

ii. providing, or causing others to provide call termination services for calls terminating in the United States or carrying any VoIP calls terminating in the United States;

iii. providing direct-inward-dial or toll-free telephone services for calls originating in the United States, including providing direct-inward-dial or toll-free phone numbers to other individuals or entities;

iv. destroying, deleting, removing, or transferring any and all business, financial, accounting, call detail, and other records concerning Defendants' operations and

the operations of any other corporate entity owned or controlled, in whole or in part, by Defendants;

B. That the Court further order, pursuant to 18 U.S.C. § 1345, that within two days from Defendants' receipt of this Temporary Restraining Order and Order to Show Cause, Defendants shall provide copies of this Temporary Restraining Order and Order to Show Cause to all of their customers for whom they provide (1) United States call termination services, (2) United States direct-inward-dial services, or (3) United States toll-free call origination services; and to all entities (a) with whom Defendants have a contractual relationship for automated or least-cost call routing, or (b) from whom Defendants acquire direct-inward-dial numbers or toll-free numbers. Within four days from Defendants' receipt of the Temporary Restraining Order and Order to Show Cause, Defendants shall provide proof of such notice to the Court and the United States, including the names and addresses or email addresses of the entities and/or individuals to whom the notice was sent, how the notice was sent, and when the notice was sent.

C. That the Court further order, pursuant to 18 U.S.C. § 1345, Somos, Inc., in its capacity as the entity designated by the Federal Communications Commission to administer the U.S. toll-free calling system and its database, to temporarily suspend all toll-free numbers registered by or on behalf of any Defendant in this matter, until further order of this Court.

D. That the Court further order, pursuant to 18 U.S.C. § 1345, that any Toll-Free Service Provider that receives notice of this Temporary Restraining Order and Order to Show Cause and has a contractual relationship with one of the Defendants in this matter to

provide toll-free numbers, shall provide to Somos, Inc. a list of all toll-free numbers provided to that Defendant that are currently active.

E. That the Court further order, pursuant to 18 U.S.C. § 1345, that any individual or entity who has obtained a toll-free number through one of the Defendants in this matter, either directly or through another intermediate entity, and wishes to continue using that toll-free number may submit a request to the Court, copying counsel for the United States, and identifying: (1) the individual or entity's name, address, phone number, email address, website URL, and the nature of their business; (2) the end-user of the toll-free number's name, address, phone number, email address, and website URL if the end-user did not obtain the toll-free number directly from Defendants; (3) the nature of the end-user's business; (4) the purpose for which the end-user utilizes the toll-free number; (5) the date on which the individual or entity obtained the toll-free number and, if applicable, provided it to the end-user; and (6) whether the toll-free number is used by the individual, entity, or end-user in connection with robocalls. The United States shall then notify the Court within four business days whether the United States has any objection to removing the specifically identified toll-free number from the list of suspended numbers.

F. That the Court issue a preliminary injunction on the same basis and to the same effect.

G. That the Court issue a permanent injunction on the same basis and to the same effect.

H. That the Court order such other and further relief as the Court shall deem just and proper.

Dated: January 28, 2020
Brooklyn, New York

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney

EVAN P. LESTELLE
BONNI J. PERLIN
Assistant United States Attorneys
United States Attorney's Office
Eastern District of New York
271-A Cadman Plaza East
Brooklyn, New York 11201
Tel: (718) 254-7000
Fax: (718) 254-6081
Evan.Lestelle@usdoj.gov
Bonni.Perlin@usdoj.gov

JOSEPH H. HUNT
Assistant Attorney General

DAVID M. MORRELL
Deputy Assistant Attorney General

GUSTAV W. EYLER
Director
Consumer Protection Branch

JILL P. FURMAN
Deputy Director

ANN F. ENTWISTLE
CHARLES B. DUNN
Trial Attorneys
U.S. Department of Justice
P.O. Box 386
Washington, D.C. 20044
Tel. (202) 307-0066
Tel. (202) 305-7227
Fax: (202) 514-88742
Ann.F.Entwistle@usdoj.gov
Charles.B.Dunn@usdoj.gov